



# Micro e Macro trend di sicurezza in Italia e nel mondo

**Alessandro Livrea**

Vice President Akamai Technologies



# Akamai Platform

## A GLOBAL PLATFORM

2023

Akamai's threat  
researchers analyze  
**454 TB**  
of new attack data  
everyday

ITALY

365,000+ servers  
1,500+ networks  
130+ countries  
4,200+ locations  
250+ Tbps of peak

7,000+ servers  
15+ networks  
60+ locations  
6+ Tbps of peak  
11+ Tbps of capacity

# Akamai Visibility in 2023

223 Billion  
Web application  
and API attacks

>18 Trillion  
Malicious bot  
requests

## Methodology

### Survey Purpose

Senior government leaders, in EMEA and beyond, are embracing technology innovation to shape the next generation of public services. Accelerated digital transformation brings heightened data protection, and operational security challenges. This survey investigates how senior civil servants are investing in cybersecurity to enhance resiliency, while enabling digital transformation.

### Sample Qualification

Conducted in 4 countries  
Organizations with 100+ employees  
National, regional and local governments  
Respondent has a role in spending on IT products and services, including IT security

### Survey Design

CATI survey conducted in August-September 2023

### Survey Topics

- Drivers and challenges of government digital transformation
- Drivers, challenges and investments in cybersecurity



N = 22



N = 27



N = 22



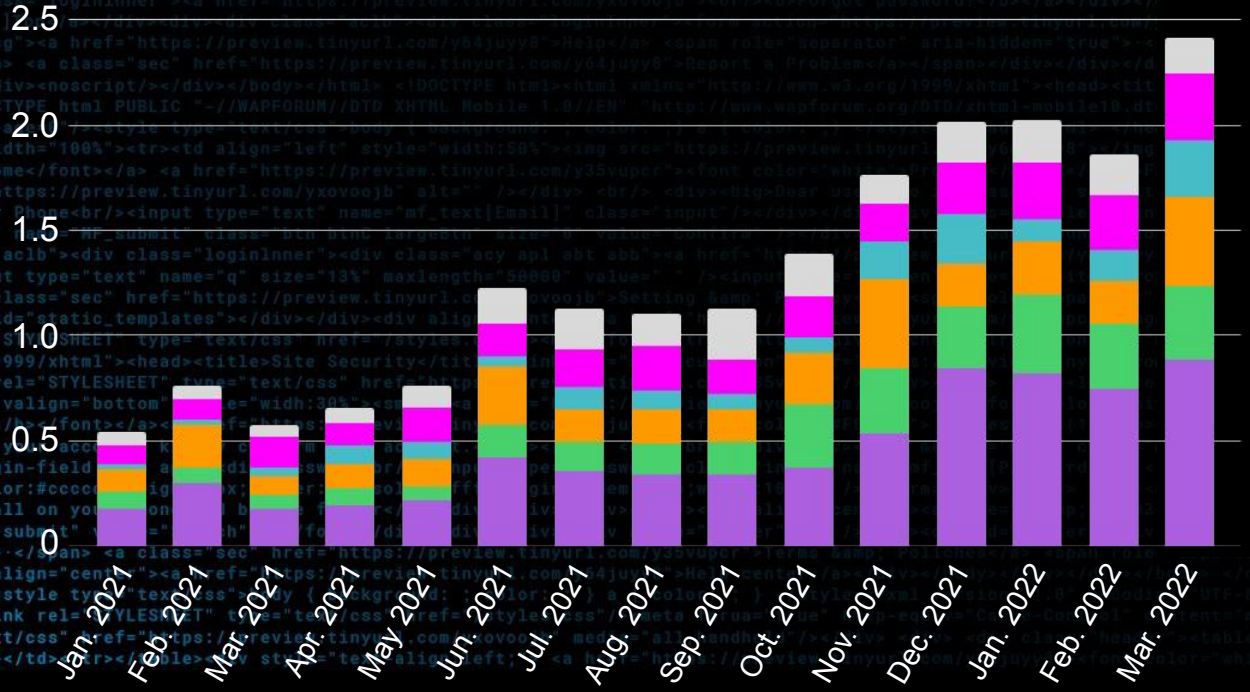
N = 29



ENR | 29

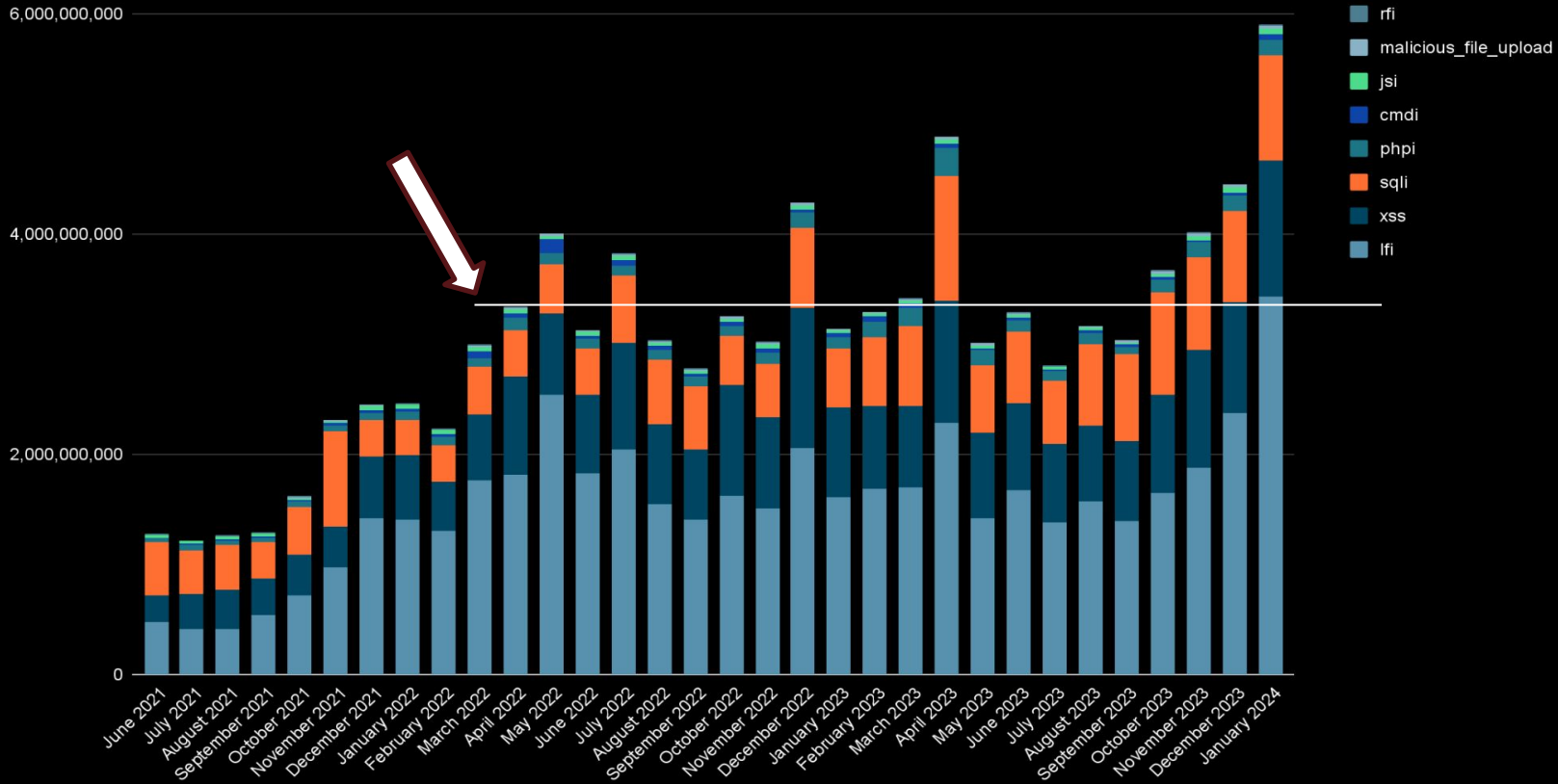
# Global Application and API Attack Traffic

Requests Per Month (Billions)



- Public
- Media
- Manufacturing
- High Tech
- Financial Services
- Commerce

# Application Attacks June 21 - January 24



# Web App and API Attacks

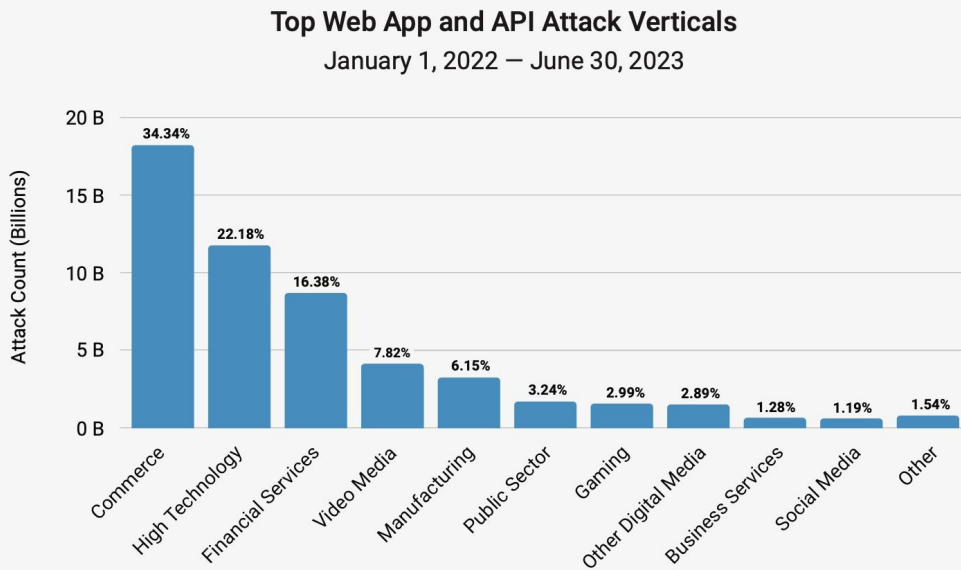


Fig. 1: Financial services remains in the third spot in web application and API attacks during the reporting period because of the industry's continued digitalization and the alarming rate in which adversaries are exploiting web application vulnerabilities in attacks

# Web App and API Attacks



## Top Web App and API Attack Vectors: Financial Services

January 1, 2022 – June 30, 2023

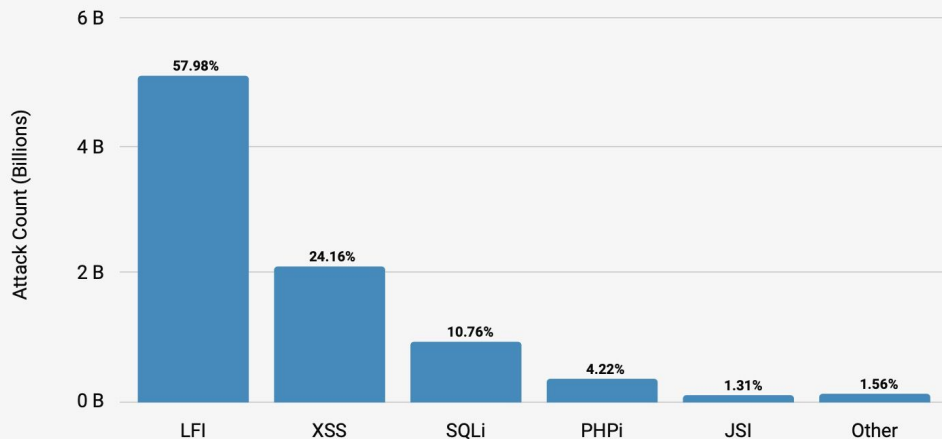


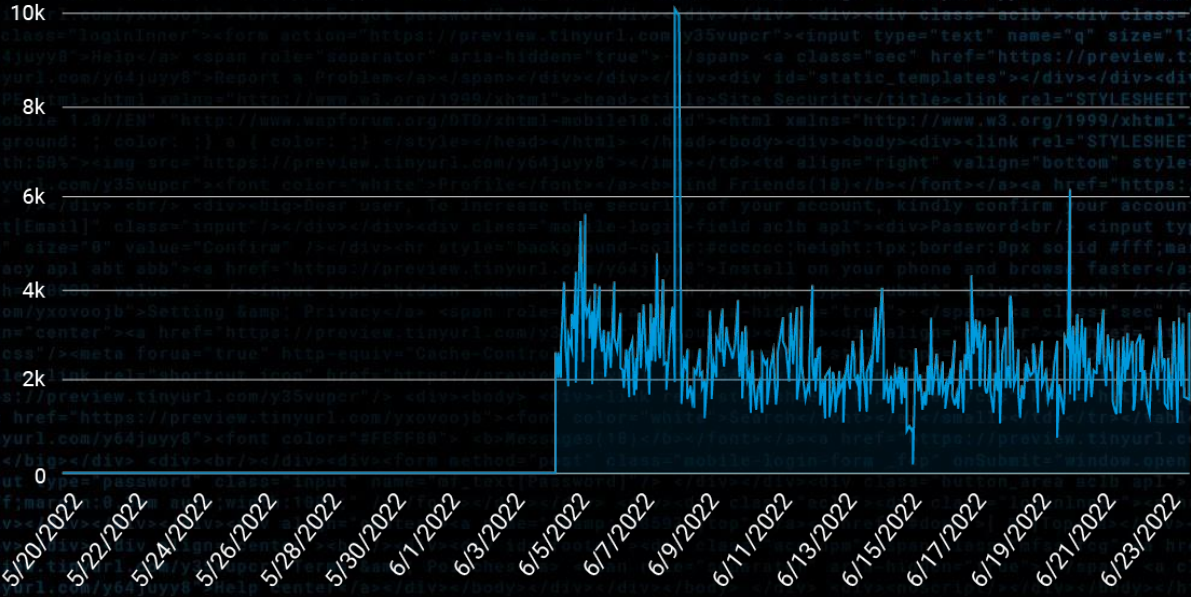
Fig. 3: LFI consistently retains the top web attack vector spot, but other vectors like SQLi, continue to pose risks to financial services



# The Perils of Emerging Vulnerabilities

Number of Exploitation Attempts (Detailed View)

Within 24 hrs after disclosure, exploitation of emerging vulnerabilities begins



\*based on our Confluence vulnerability research



# Web App and API Attacks

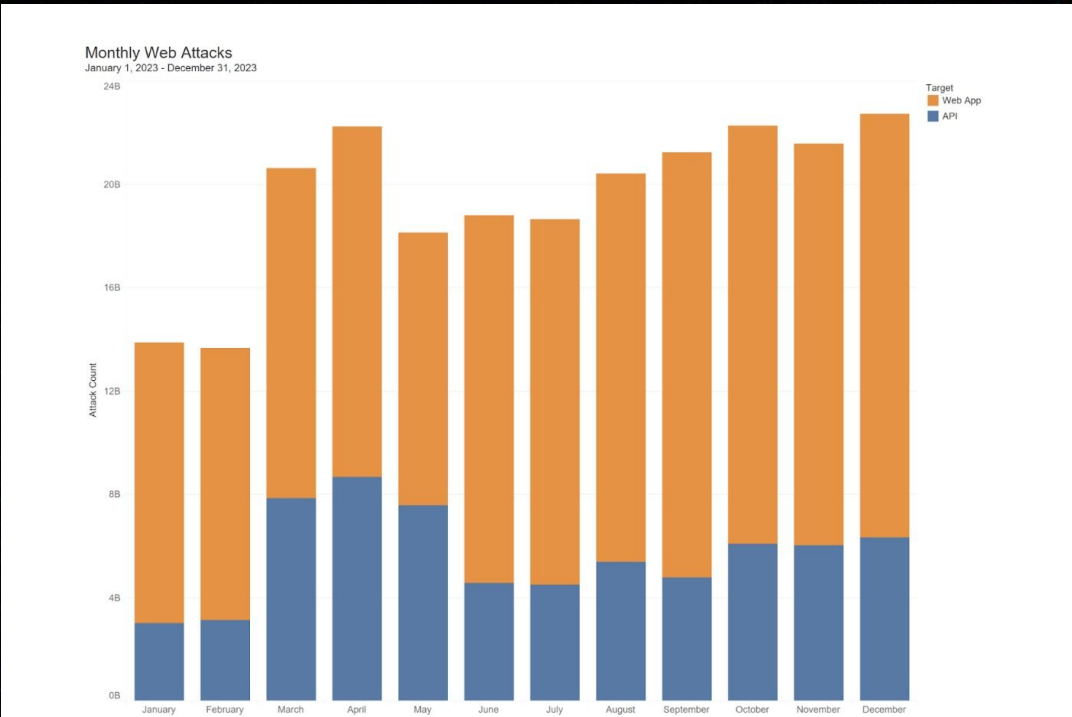
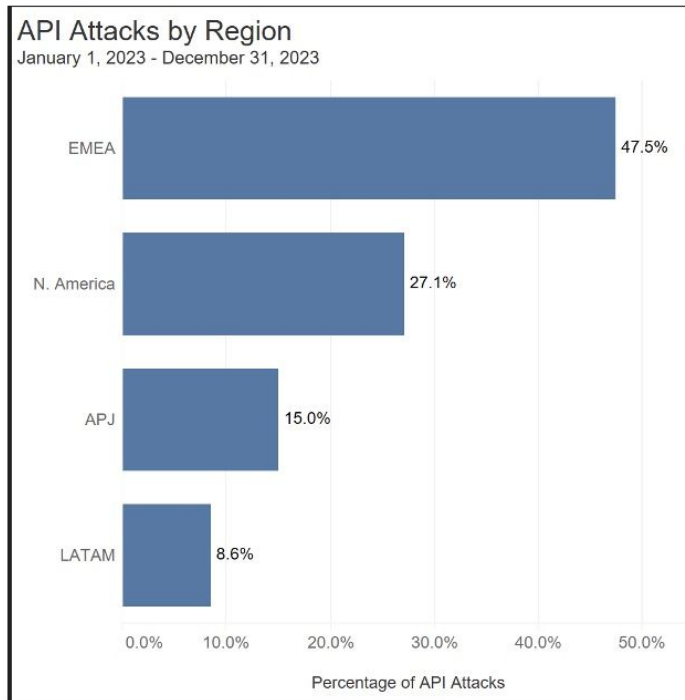


Fig. 1: Web attacks against APIs spiked from 22% in January to 28% in December, with several fluctuations between March and May 2023

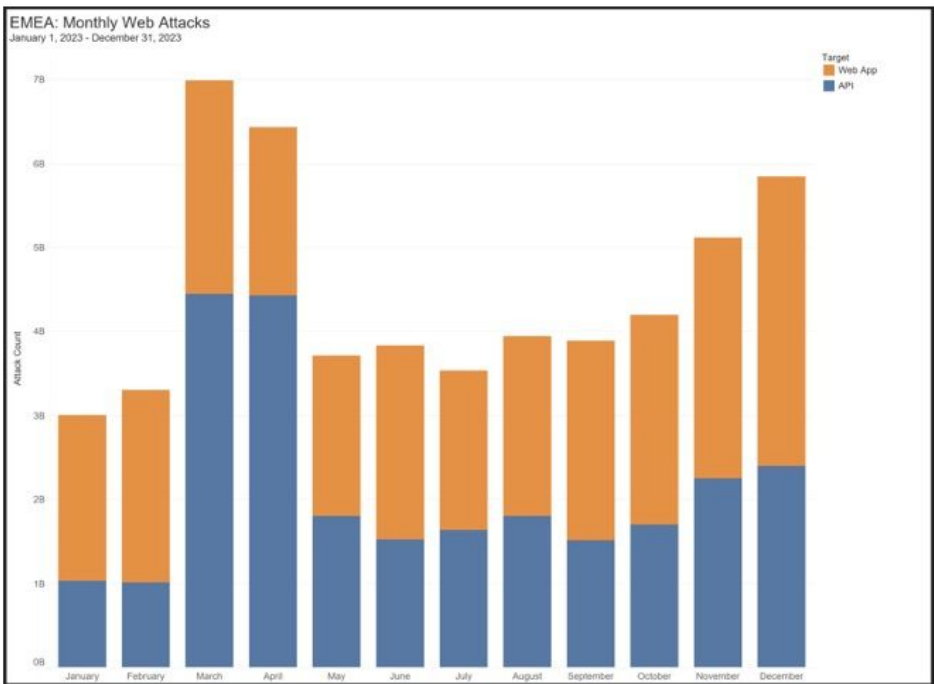


# API Attacks by region



EMEA Fig. 1: Web attacks are significantly more likely to target APIs in EMEA than in any other region

# EMEA Web APP and API Attacks



EMEA Fig. 2: With the exception of March and April, when API attacks spiked, API attacks increased steadily during 2023, rising to 41% of all attacks by the end of the year

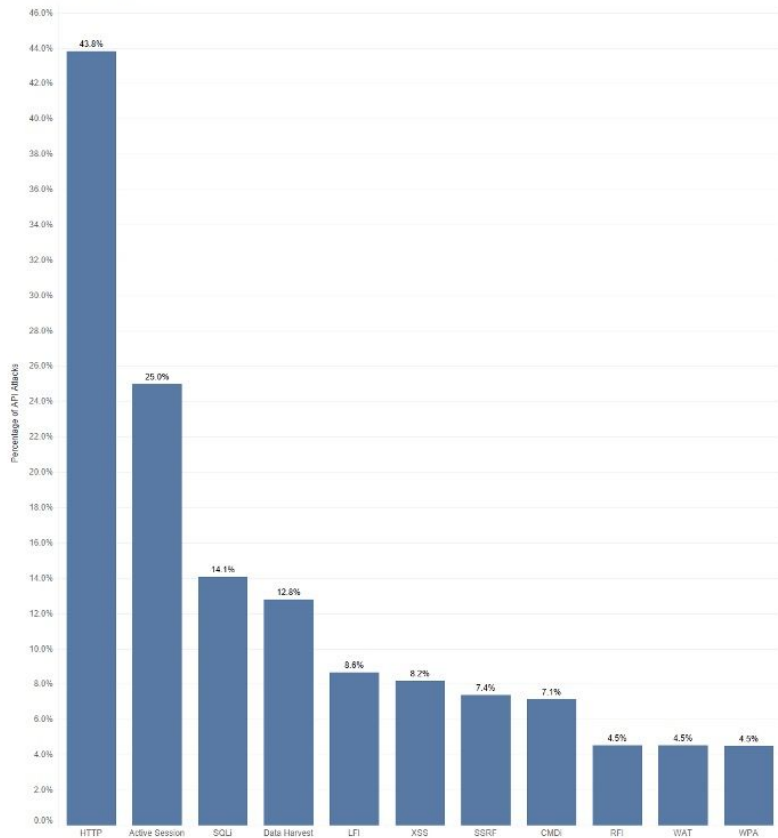


Fig. 2: Although Local File Inclusion (LFI) is not the top vector in APIs, it's still an area of concern as it can be used to infiltrate intended targets; a closer look at the distribution of attacks for both web applications and APIs, however, reveals LFI is still one of the top attack vectors

# API Attacks by Vectors

# General Ransomware Killchain



**Initial Foothold**

(Spear) Phishing or vulnerable exposed applications



**Lateral Movement**

Spread across the network for maximum coverage



**Exfiltration**

Find and steal valuable data



**Encryption**

PKI with encryption to prevent cracking



**Ransom Note**

Wallpaper and ransom txt file



**Profit**

# Ransomware

## Average number of ransomware attacks over the past 12 months by country

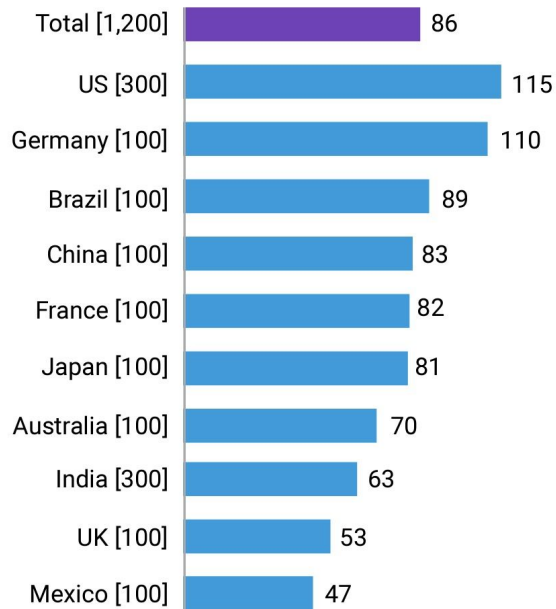


Fig. 1: How many ransomware attacks has your organization been targeted with in the last 12 months (regardless of whether they were successful or not)? [1,200], only showing the average number

# Ransomware

## Impact of ransomware/cyberattacks

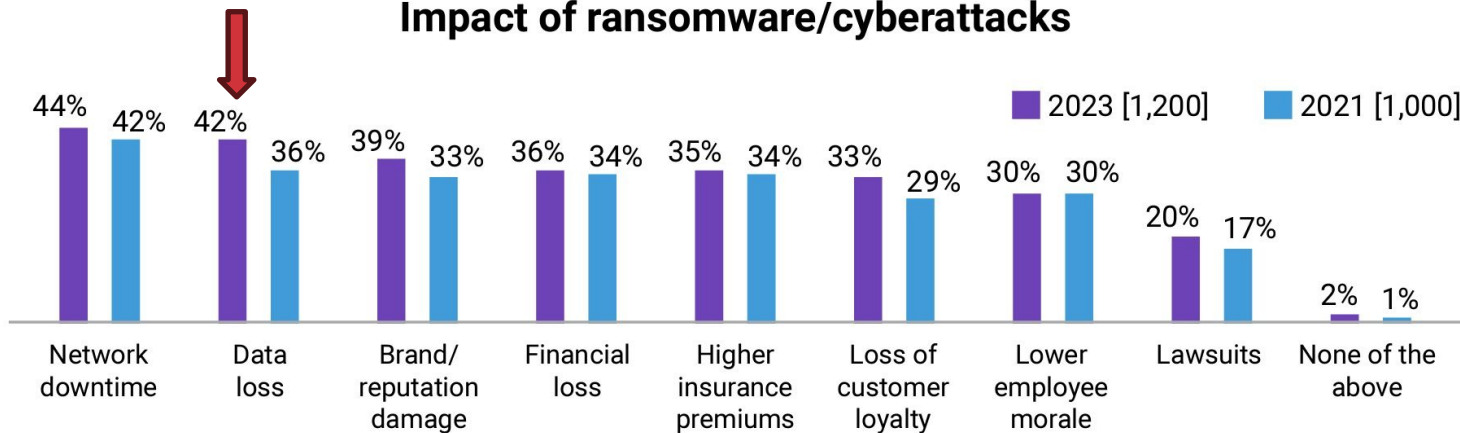
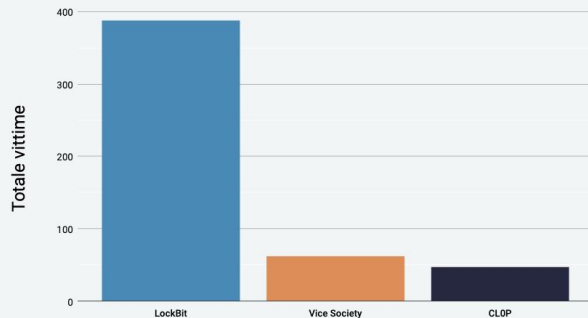


Fig. 3: When your organization has previously detected ransomware or some other cyberattack, which of the following impacts has it had on your organization? [Base sizes in chart], not showing all answer options, split by historical data.

# Ransomware

EMEA: i primi 3 gruppi di ransomware per numero di vittime

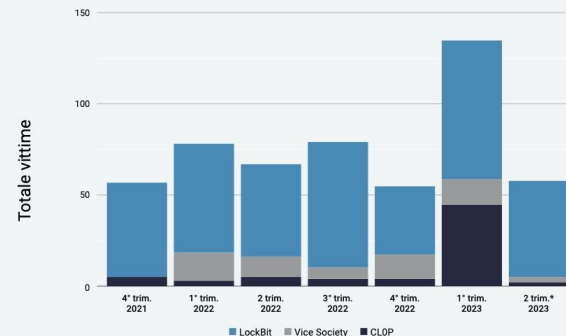
1° ottobre 2021 - 31 maggio 2023



EMEA - Figura 1. La maggior parte delle organizzazioni che hanno subito attacchi di ransomware nell'area EMEA è stata colpita dai gruppi LockBit, Vice Society e CLOP

EMEA: i primi 3 gruppi di ransomware per numero di vittime

Trimestrale: 1° ottobre 2021 - 31 maggio 2023



EMEA - Figura 2. Confronto trimestrale del numero di aziende vittime dei tre principali gruppi di ransomware nell'area EMEA: LockBit, Vice Society e CLOP



# Ransomware

**THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT**

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.

We can confirm that Lockbit's services have been disrupted as a result of International Law Enforcement action – this is an ongoing and developing operation.

Return here for more information at:

11:30 GMT on Tuesday 20th Feb.

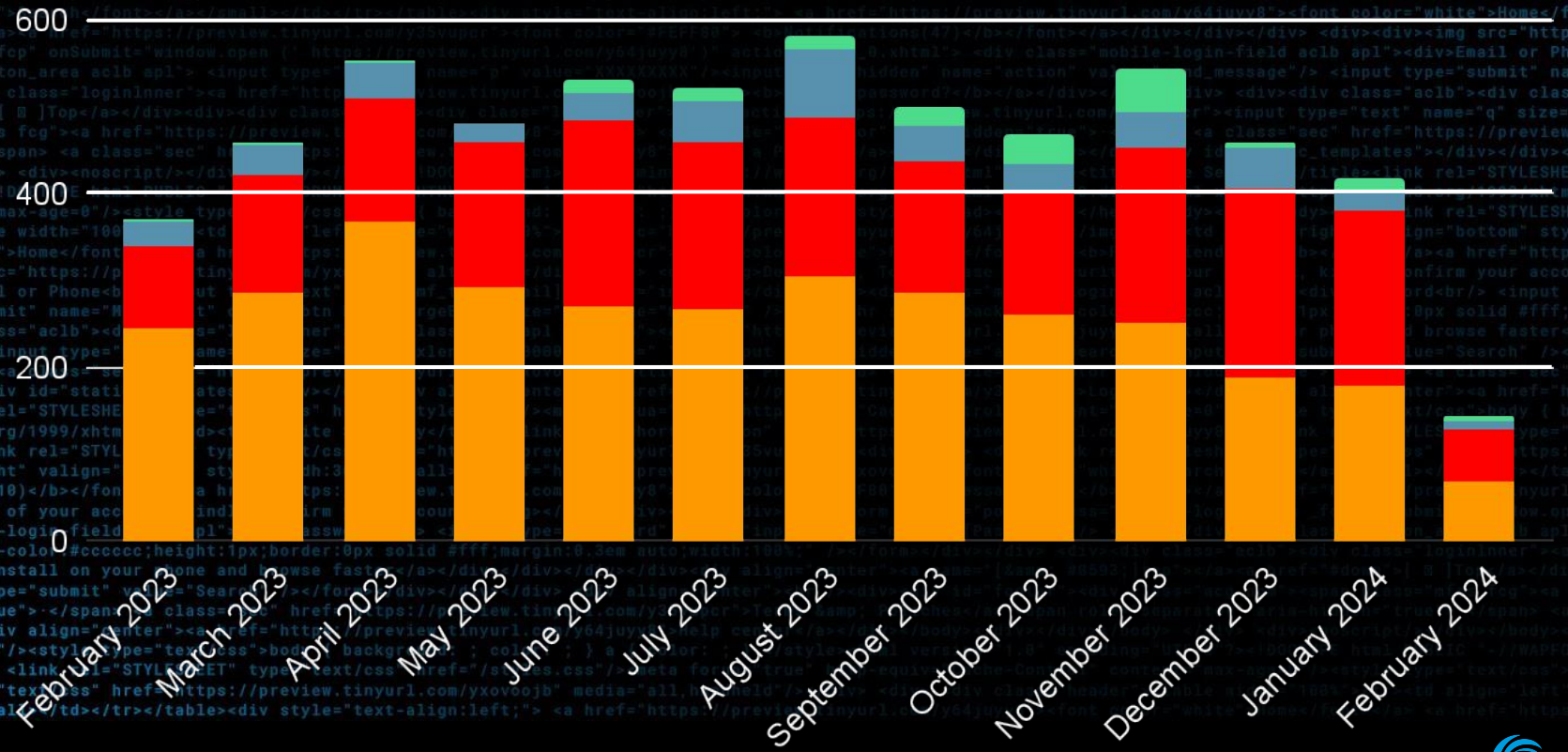
**LOCKBIT**

NCA National Crime Agency, ROCU, EUROPOL, POLITIE, Kanton Zürich, Carabinieri, SH, POLIISI, and various police department crests.

Fig. 2: The announcement of the systemic disruption of the largest and most prolific RaaS group and its affiliates

# Global DDoS Attacks

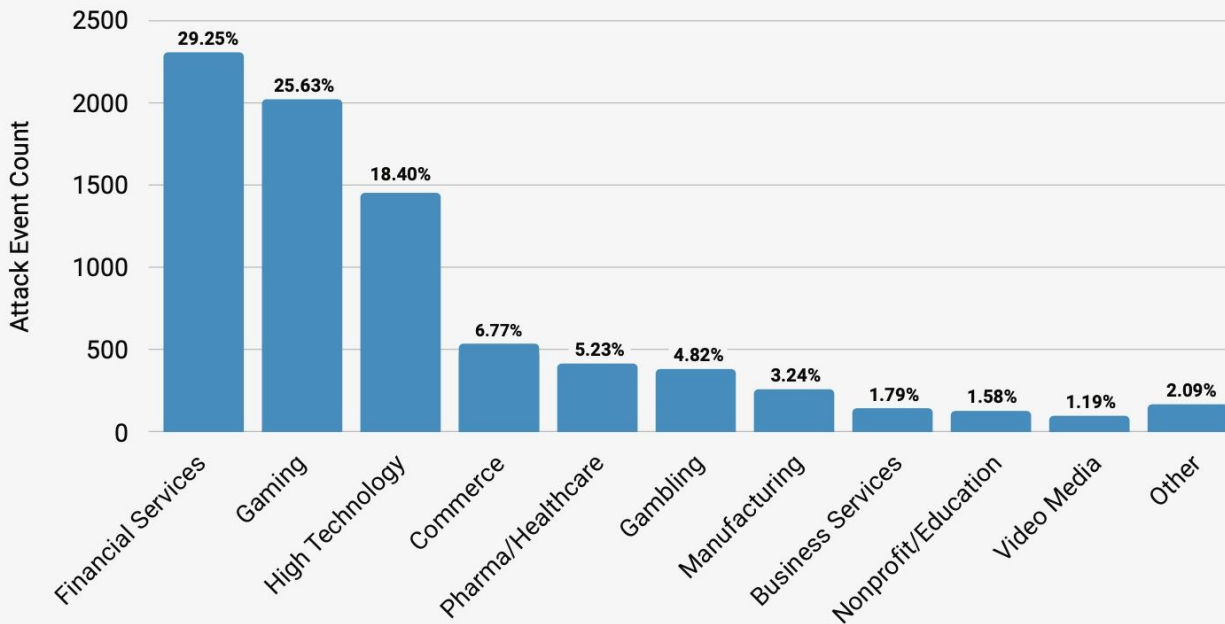
LATAM APJ EMEA N. America



# Regional Data: DDoS Attacks

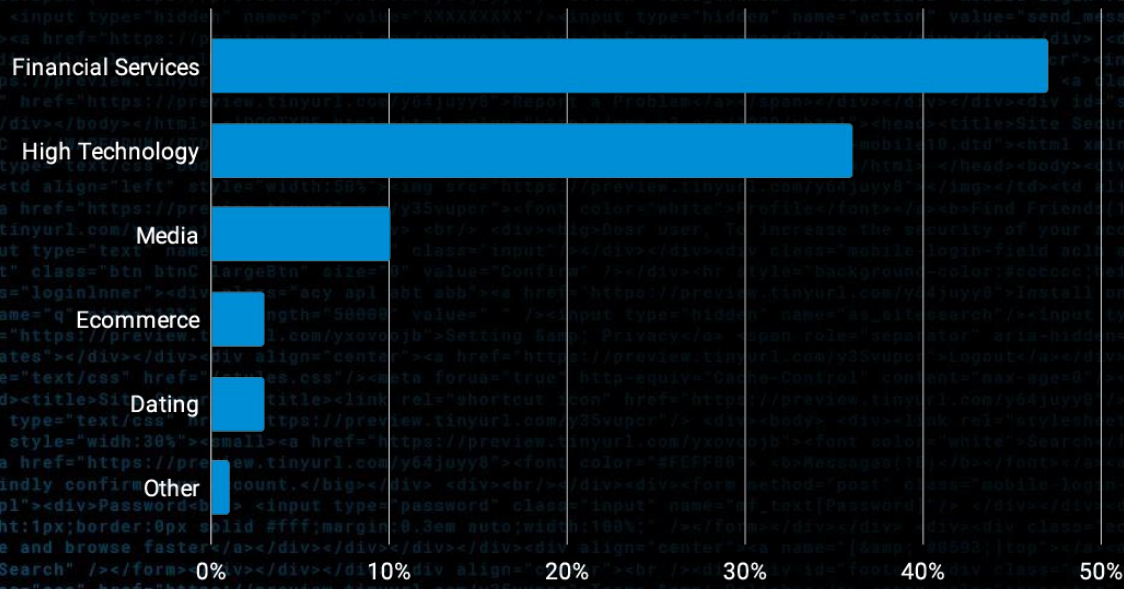
## Top DDoS Attack Event Verticals

January 1, 2022 – June 30, 2023



# Phishing Trends

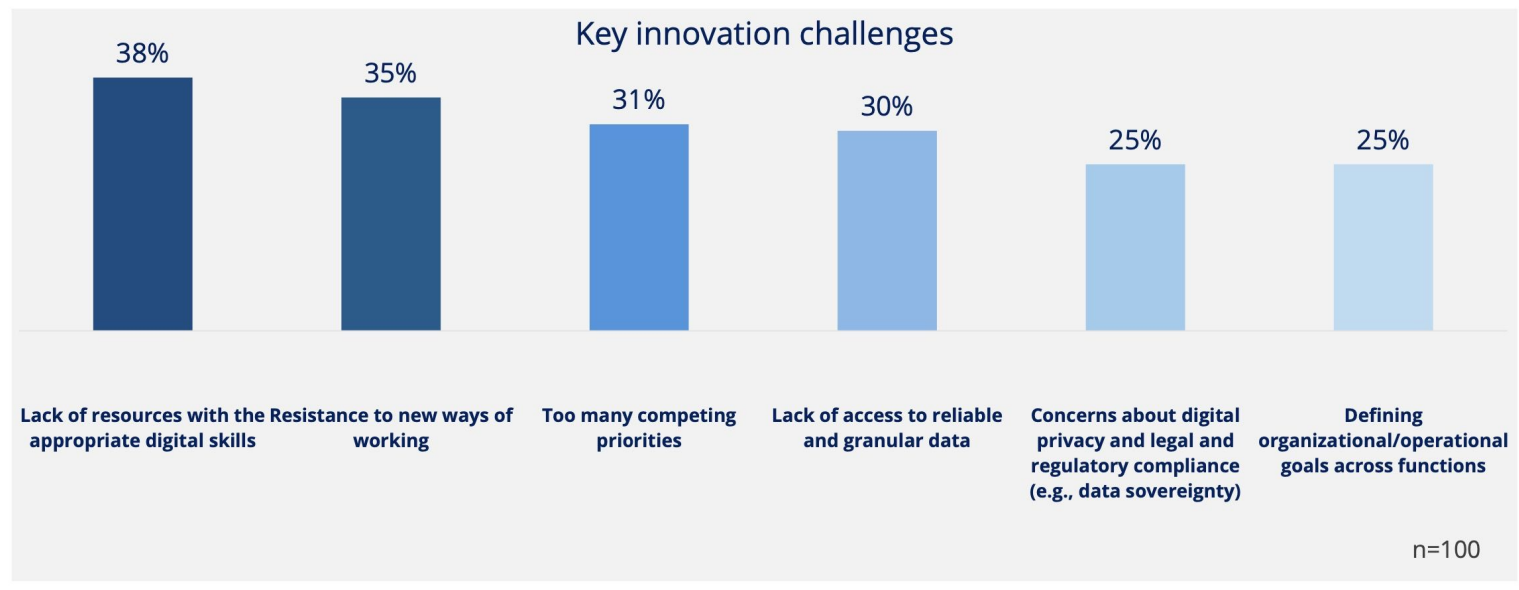
## Phishing Attacks by Industry



# Ostacoli all'innovazione nella Pubblica Amministrazione

European senior government leaders understand that organizational challenges are the main obstacles to innovation

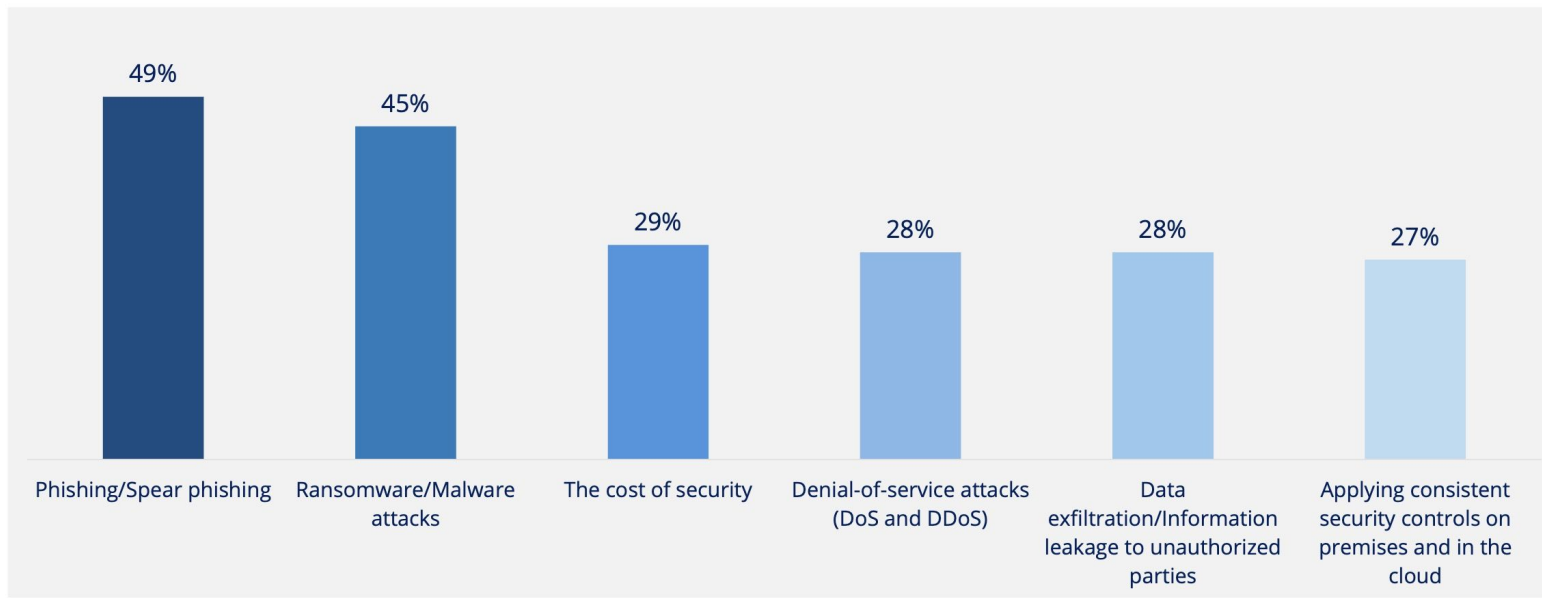
## What are the main obstacles to your innovation plans?



# Principali sfide di sicurezza

Phishing and ransomware are the most common security issues, faced by European governments

Which of the following security challenges have you encountered in the past year? [Choose all that apply]



# Priorità

The top IT security operational priorities for European government senior leaders is compliance with data privacy, digital sovereignty and other regulatory requirements

## What are your IT security team's top operational priorities? [Choose up to 3]

### IT security operational priorities



# Conclusions

Review your APP & API risks, as threat is focused on them

Prevent Lateral Movements







GRAZIE



Intelligent Security Starts at the Edge